



# UNITED STATES PATENT AND TRADEMARK OFFICE

80  
UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
08/949,525	10/14/1997	MICHAEL J. WIENER	ENT970827-1	8206
7590	03/28/2005			EXAMINER PYZOWCHA, MICHAEL J
CHRISTOPHER J RECKAMP Vedder Price Kaufman & Kammholz 222 North LaSalle Street Suite 2600 Chicago, IL 60601			ART UNIT 2137	PAPER NUMBER
DATE MAILED: 03/28/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	08/949,525	WIENER ET AL.
	Examiner	Art Unit
	Michael Pyzocha	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 28 February 2005.
- 2a) This action is **FINAL**.                                   2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-3,5-17,19-23 and 25-30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-3,5-17,19-23 and 25-30 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) All   b) Some \* c) None of:
  1. Certified copies of the priority documents have been received.
  2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: \_\_\_\_\_.

**DETAILED ACTION**

1. Claims 1-3, 5-17, 19-23 and 25-30 are pending.
2. Amendment filed 02/28/2005 has been received and considered.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over McDonald et al ("A Socket-Based Key Management API (and Surrounding Infrastructure)") and further in view of Schneier (Applied Cryptography).

As per claim 9, McDonald et al discloses providing, through a multi-client manager unit (see page 2), selectable expiry data including public encryption key expiry data associated with a public encryption key that is selectable on a per client basis (see page 3 where "protocol addresses are used as an index" shows a per client basis); digitally storing selected public

Art Unit: 2137

encryption key expiry data for association with a new encryption key pair; generating a new encryption key pair and associating the stored selected expiry data with the new encryption key pair to affect a transition from an old encryption key pair to a new encryption key pair (see page 3).

McDonald et al fails to disclose the new encryption key pair is not computable from a previous encryption key pair.

However, Schneier teaches generating new encryption keys that are not computable from a previous key (see pages 45-46).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Schneier's method of generating keys to generate the key pairs in McDonald et al.

Motivation to do so would have been to provide a cryptographically secure key (see Schneier pages 45-46).

5. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified McDonald et al and Schneier system as applied to claim 9 above, and further in view of RFC 2137.

As per claim 10 the modified McDonald et al and Schneier system fails to disclose the method of providing, generating, storing, and associating digital signature key pairs as well as the encryption key pairs.

However, RFC 2137 teaches the updating of digital signature key pairs (see pages 8-9).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the modified McDonald et al and Schneier system to also updating digital signatures as in RFC 2137.

Motivation to do so would have been that an update of a key would invalidate the digital signature (see RFC 2137 page 9).

***Allowable Subject Matter***

6. Claims 1-8 and 14-30 are allowed. Reasons for allowance include, for example in claim 1, the last two paragraphs; particularly the steps of receiving a new digital signature key pair from the client and creating a new digital signature certificate.

7. Claims 11-13 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Response to Arguments***

8. Applicant's arguments filed 02/28/2005 have been fully considered but they are not persuasive. Applicant argues the

Art Unit: 2137

cited portion is silent as to any selectable expiry data namely public encryption key expiry data associated with a public encryption key that is selectable on a per client basis.

However, the cited page 3 of 7 discloses selectable expiry data where under KEY\_UPDATE the lifetime sets when the key will expire. See also KEY\_ADD, which refers back to page 2 of 7; paragraph 3 where it also discusses key lifetime. Also in paragraph 3 there is a discussion of how the security association exists between two communication endpoints, which means it is different for each connection. Additionally in paragraph 3 McDonald teaches the use of public keys.

#### ***Conclusion***

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Application/Control Number: 08/949,525  
Art Unit: 2137

Page 7

MJP

*Andrew Caldwell*  
ANDREW CALDWELL  
SUPERVISORY PATENT EXAMINER